Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report for 30 July 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- NBC reports two 55−gallon drums of toxic waste, illegally dumped, were discovered along an Ohio road; one was leaking toxic fluid. (See item 2)
- The New Mexico Channel reports a bomb scare sent Albuquerque police scrambling after a small device exploded in a resident's mailbox. (See item 19)
- Check Point Software Technologies issued a patch on Wednesday to fix vulnerabilities which may cause a buffer overrun, potentially compromising the gateway. (See item 40)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 29, The Arizona Republic* — **Arizona refinery project facing approval process. The first new U.S. oil refinery in decades could be opened near Yuma, AZ, in late 2008. That's assuming proponents, who already have invested five years in the project, are able to surmount some pretty formidable obstacles. The Arizona Clean Fuels Refinery is the only active new refinery project in the United States,** despite industry claims that current facilities are now operating at capacity with demand increasing every year. Proponents of the $2.5 billion project, which has been relocated from Maricopa to Yuma County, hope to receive a draft air−quality permit from the Arizona Department of Environmental Quality in the next month. After that there will be a series of public hearings on the proposed permit and an eventual final

decision. An Environmental Protection Agency permit also is necessary and hinges on the state's approval. The refinery would have an output capacity of 150,000 barrels, or 6.3 million gallons of gasoline, more than enough to cover Phoenix, AZ's, average daily supply of 4.6 million gallons.
Source: http://www.azcentral.com/arizonarepublic/business/articles/0_729refineryside29.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *July 29, NBC 4 Columbus (OH)* — **Barrels of hazardous waste found along Ohio roads.** Two 55−gallon drums of toxic waste were discovered Wednesday, July 28, along a Mansfield, OH, road. One was leaking toxic fluid. The substance spilled into a creek that flows into the Rocky Fort River. **Officials have no idea how much of the substance leaked into the creek, according to Dina Pierce of the Ohio Environmental Protection Agency (EPA). Since June, the Ohio EPA has documented at least six areas in Mansfield where chemicals have been illegally dumped and are trying to find out where they originated.** Mansfield fire officials said the actual number of illegal chemical dumpings is twice as high.
Source: http://www.nbc4columbus.com/news/3592109/detail.html

3. *July 29, KSLA TV (LA)* — **Chemical leak sends people to the hospital, forces evacuations.** Police evacuated about 50 homes and a motel in Mt. Pleasant, TX. Police say a truck hauling about 1,800 gallons of hydrochloric acid through the Texas town began leaking. **Along with the evacuations, the entrance ramps from Interstate 30 into Mt. Pleasant were closed. Hazmat crews have arrived at the scene.** There is also information that some of the acid got into a nearby creek, killing a number of fish.
Source: http://www.ksla.com/Global/story.asp?S=2107103&nav=0RY4PKE8

[Return to top]

Defense Industrial Base Sector

4. *July 29, Department of Defense* — **DoD approves Army plan to reach out to sailors, airmen. The Department of Defense (DoD) announced on Thursday, July 29, that sailors and airmen are now able to "Go Army" under a new program intended to rebalance the size of the military.** The program will generate new opportunities for continued service and career advancement for those willing to transfer into the Army from other services. Under "Operation Blue to Green," the Army will reach out to sailors and airmen and underscore the advantages of swapping their present uniform for Army green. Among them is the faster pace of Army promotions. The Army plans to use bonuses to stimulate the needed accessions and to carefully guide the experience mix so that promotions stay strong. The focus of the effort centers on grades E1−E5, but other grades will be considered in meeting Army needs. For example, the Army will continue to have a sizeable demand in the areas of law enforcement, health care, communications and intelligence. **The Army's recruiting goal for the next fiscal year is about 80,000. Of that number, the Army hopes to recruit at least 8,000 prior service troops.**

Source: http://www.dod.mil/releases/2004/nr20040729−1068.html

5. *July 29, Aerospace Daily & Defense Report* — **Fleet of hunter/killer planes would see initial use in FY '07. The U.S. Air Force is asking industry for input on the idea of procuring a fleet of as many as 60 hunter/killer remotely operated aircraft (ROA) that would fly 30−hour unmanned missions of up to 50,000 feet with 3,000 pounds of bombs. The first would become operational by late fiscal year 2007.** Each air vehicle would cost about $10 million. "The timelines are driven primarily by the global war on terrorism and the need to rapidly field supportable, affordable capabilities that are effective, flexible, and responsive to a quickly changing world situation," said a Thursday, July 22 FedBizOpps notice from the Air Force's Aeronautical Systems Center at Wright−Patterson Air Force Base, OH. The vehicle must be able to transfer information and imagery to ground centers by line of sight and global beyond line of sight, "and provide a means for positive navigation and command and control ... throughout its operating envelope and in any operational environment likely to be encountered." It will "be deployable for worldwide operations, capable of launch and recovery from a bare base, and include appropriate command and control links to operate a deployed aircraft from a fixed site," the notice said.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/kil07294.xml

6. *July 28, Government Accountability Office* — **GAO−04−858: Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation (Report).** The Department of Defense (DoD) is in the midst of transforming military capabilities. The transformation relies in part on the Global Information Grid (GIG), which is focused on building a new Internet−like network capability that DoD envisions will enable weapons and other systems and people to share information quickly, allowing warfighters to identify threats more effectively and to respond with greater precision and lethality. DoD plans to spend at least $21 billion through 2010 to build a core GIG capability. **The Government Accountability Office (GAO) was asked (1) to describe the GIG, including the concept, key acquisitions, and implementation and (2) to identify significant challenges facing DoD in implementing the GIG.** GAO is not making recommendations in this report as this effort is focused on providing an initial overview of the GIG and challenges. GAO's future work will continue to assess how DoD is addressing challenges and the progress of key acquisitions. DoD provided technical comments on this report are incorporated where appropriate. Highlights: http://www.gao.gov/highlights/d04858high.pdf
Source: http://www.gao.gov/new.items/d04858.pdf

[Return to top]

Banking and Finance Sector

7. *July 29, Finextra Research* — **CIBC accounts hit by system glitches. The Canadian Imperial Bank of Commerce (CIBC) is working to fix a computer glitch that caused transactions to be billed twice on 60,000 customer accounts. CIBC says personal line of credit accounts were affected by a system error that resulted in the duplication of transactions that customers had undertaken** over the weekend or on Monday, July 26. CIBC says the computer systems responsible for processing transactions are now operating normally.

According to local press reports, President's Choice Financial, which is operated by CIBC subsidiary Amicus Bank, was also hit by system problems which prevented customers from viewing balances and transactions after logging on to online services. The system failures at CIBC follow others at the Royal Bank of Canada (RBC) last month where problems arising during a routine software upgrade caused payroll delays for thousands of workers.
Source: http://www.finextra.com/topstory.asp?id=12260

8. *July 29, Associated Press* — **Credit companies resist anti−identity theft freeze.** One weapon against identity theft is gaining currency, but few people know about it. It is called the security freeze, and it lets individuals block access to their credit reports until they personally unlock the files by contacting the credit bureaus and providing a PIN code. **The process is a bit of a hassle and only available in certain states, and the credit−reporting industry believes it complicates things unnecessarily. However, it appears to be one of the few ways to virtually guarantee that a fraudster cannot open an account in your name.** With identity theft apparently growing, the advocates hope the freeze gains national momentum. While the freeze may be an extreme step, its backers say it is necessary because the existing system is broken. The Internet and consumer databases have made it easier than ever to find someone else's social security number and apply for accounts in that name. The industry has fought the freeze, contending that fraud alerts and new protections in last year's federal Fair and Accurate Credit Transactions Act offer significant defense against identity theft.
Source: http://www.dfw.com/mld/startelegram/news/state/9273689.htm?1_c

9. *July 29, News24.com (South Africa)* — **It was only phishing according to eBay. The world's largest auction Website, eBay, on Wednesday, July 28, confirmed that a compromised database with user data did not come from its servers, saying they believe the information in the hands of South African police was the result of phishing efforts.** News24 and sister newspaper Beeld earlier this week reported that South African police were advising users who had transacted on eBay to "cancel their credit cards immediately following the hacking of an eBay database." Hani Durzy, eBay spokesperson, said "this information clearly came from phishing efforts and not from eBay's servers." This view was supported by the U.S. Embassy in Pretoria saying, "we can confirm that the data in possession of the South African police was obtained from "phishing" and not from a hack on eBay's servers." Director Lesley Magson, commander of the South African Police Service's commercial crimes unit in Johannesburg, said that police had considered "phishing" as a cause, but were not convinced as there was no single e−mail or Website visited by the compromised users' which would have tied them together.
Source: http://www.news24.com/News24/South_Africa/News/0,,2−7−1442_1 564859,00.html

10. *July 29, Ros Business Consulting News (Russia)* — **Putin signs bill on fighting money laundering.** Russian President Vladimir Putin has signed a federal bill on fighting money laundering and terrorism financing, the press service of the President reported. The bill was approved by the State Duma on July 7, and by the Federation Council on Thursday, July 15. In particular, the bill broadens the list of entities that must submit corresponding information to authorized agencies. The list includes real estate agencies, lawyers, notary officers, and entrepreneurs that provide legal assistance and accounting services. **According to the bill, information about suspicious deals must be submitted to law enforcement agencies only if there are grounds to believe that such deals are aimed at laundering money and financing terrorism.**

Source: http://www.rbcnews.com/free/20040729101825.shtml

11. *July 28, Government Computer News* — **New tool demonstrates hacks against RFID tags. Smart−tag technology using radio frequency ID (RFID) is being developed without security in mind, raising concerns about consumer privacy and risks to security of the organizations using the tags.** Some of these risks were demonstrated on Wednesday, July 28, at a security conference in Nevada using a new hacker tool that lets users read and write to the tags. **The problem is that the 128 bytes of data on most tags are visible to anyone with a reader. No tags now are read−protected, and few are write−protected.** Lukas Grunwald, CTO of DN−Systems Enterprise Internet Solutions of Germany, demonstrated a beta version of RF−DUMP, software that runs on a notebook or personal digital assistant, that lets the user read and write to most standard smart tags. The software would let customers rewrite tags in a store. Stores also could rewrite tags to ID customers by associating a purchase with credit card information, creating a wearable personal cookie that could be used to track someone in a store. Grunwald warned that dependence on an unsecure technology could put users at risk, and creation of a new critical infrastructure could open a new avenue of attack for terrorists. Source: http://www.gcn.com/vol1_no1/daily−updates/26759−1.html

12. *June 29, Government Accountability Office* — **GAO−04−882R: Better Information Sharing Among Financial Services Regulators Could Improve Protections for Consumers (Report).** As regulators are faced with the challenges of overseeing a myriad of financial products, along with the individuals and organizations that develop and sell them, information sharing among regulators serves as a key defense against fraud and market abuses. However, the system of financial regulation is fragmented and, in many cases, isolated among numerous federal and state financial regulators overseeing the securities, insurance, and banking industries. **While there has been a greater effort to improve communication in recent years, the routine sharing of information between the regulators of the three major financial industries −− securities, insurance, and banking −− continues to be a source of concern.** At Congress' request, the Government Accountability Office has issued reports and testimonies in recent years discussing the benefits of improved sharing of criminal and regulatory information and the consequences of failing to adequately share such information. **This report focuses on three areas where greater attention is needed to improve information−sharing capabilities among financial services regulators.** Abstract: http://www.gao.gov/docsearch/abstract.php?rptno=GAO−04−882R.
Source: http://www.gao.gov/new.items/d04882r.pdf

[Return to top]

Transportation Sector

13. *July 29, Newsday.com* — **MTA eyes fare hike, service cuts for LIRR.** The Metropolitan Transportation Authority (MTA) is considering raising Long Island Rail Road (LIRR) fares by five percent and reducing off−peak service to help close its multimillion−dollar budget deficit, Newsday has learned. Among the options under consideration are fare hikes for the commuter rails, which include the LIRR and MetroNorth, and LIRR schedule changes that could mean combining a number of trains, according to a source familiar with the plan. The railroad also may cut back on train service during the non−rush hours. The MTA raised LIRR fares by an

average of 25 percent last year and the subway fare to $2. The MTA also increased tolls by 25 cents to $1 on nine city−area bridges and tunnels. MTA officials are looking at raising those tolls again. **The MTA's gaps are due to rising debt service on bonds to pay for increased borrowing, plus growing pension, benefit and employee health costs.**
Source: http://www.newsday.com/news/local/longisland/ny−lilirr293909667jul29,0,2454833.story?coll=ny−topstories−headlines

14. *July 29, Associated Press* — **Train derailment forces evacuation in Minnesota. Dozens of residents of Balaton, in southwestern Minnesota, were told to leave their homes around midnight Tuesday, July 27, after a train derailed and spilled at least 40,000 gallons of flammable ethanol.** Two rail cars from a Dakota Minnesota & Eastern train went off the tracks about 11 p.m. Tuesday. Officials at the scene suspected there was a leak in a third ethanol tanker and said a fourth tanker carrying soybean oil was also damaged. About 75 residents in a three−block radius from the derailment were evacuated. Fifty of them spent the remainder of the night in the library at the Balaton Public School while the others were able to stay with relatives or friends. No one was hurt. The 75−car train was going east when it derailed near a ditch that drains into Lake Yankton. The leaking chemicals were held behind quickly built dikes, said Craig Shafer of the Minnesota Pollution Control Agency. He estimated nearly all the 30,000 gallons of ethanol in one tanker had leaked and another 15,000 gallons from a second tanker. The possible leak in a third tanker was smaller, he said.
Source: http://www.duluthsuperior.com/mld/duluthsuperior/9262046.htm

15. *July 29, Department of Transportation* — **DOT makes $25 million loan to regional railroad.** The Wheeling & Lake Erie (W&LE) Railway will get a much needed face lift thanks to a new loan from the Department of Transportation (DOT) meant to boost the competitiveness of the railroad that serves as a key economic link in Ohio, Pennsylvania, and West Virginia. **Assistant Secretary for Transportation Policy Emil Frankel was on hand at the railroad,s Brittain Yard in Akron on Thursday, July 29, to announce a $25 million loan to the W&LE for rehabilitation of 315 miles of track and replacement of over 168,000 rail ties.** The loan is provided through the Department's Railroad Rehabilitation and Improvement Financing (RRIF) program. The infrastructure improvements will enhance the ability of the W&LE to move freight using 286,000 pound rail cars, now the industry standard, and continue providing its approximately 170 customers competitive shipping rates and a cost−effective alternative to commercial truck service. **The W&LE is a regional railroad that provides common carrier rail service over approximately 900 miles in 23 counties located in Ohio, Pennsylvania, West Virginia, and Maryland.** It connects with three Class I railroads and 14 short line railroads, and primarily carries commodities such as coal, stone, iron ore, and steel.
Source: http://www.dot.gov/affairs/dot11104.htm

16. *July 29, Associated Press* — **Airport screeners caused longer waits.** The federal security director at Arizona's largest airport has been placed on administrative leave by the Department of Homeland Security amid a newspaper report about passenger screening. **The Arizona Republic reported Wednesday, July 28, that federal authorities responsible for security at Phoenix's Sky Harbor International Airport intentionally lengthened wait times at passenger checkpoints at a time when they were asking Homeland Security administrators in Washington to provide more screeners.** Transportation Security Administration (TSA) officials denied the move was an attempt to manipulate staffing to get

more positions approved. TSA officials confirmed that Marcia Florian was placed on administrative leave Tuesdaym July 27, and temporarily replaced by Randal Null, who had been in charge of aviation operations in Washington. The e−mails written by Fred Carter, screening chief at Sky Harbor, to Florian alerted staffers to the wait−time move on April 5. "My initial goal is to man our checkpoints to about a 15−min wait time," Carter wrote. **Fifteen minutes of waiting is nearly triple the average time that passengers spent in checkpoint lines at Sky Harbor, which is the nation's fifth−busiest airport.** Last week, Florian said the e−mails reflected a plan to deal with staffing shortages, not to dupe headquarters into approving additional workers.
Source: http://www.zwire.com/site/news.cfm?newsid=12534680&BRD=1817&PAG=461&dept_id=222076&rfi=6

17. *July 27, Transportation Security Administration* — **TSA purchases thirty−seven explosives detection machines. The Transportation Security Administration (TSA) today announced it has purchased 37 eXaminer 6000 Explosives Detection System (EDS) machines. This is in addition to the approximately 460 L−3 EDS machines already in use screening checked luggage at the nation's airports.** "TSA is purchasing these machines for permanent in−line checked baggage screening solutions that the agency is developing in partnership with various airports," said Rear Adm. David M. Stone, USN (Ret.), Assistant Secretary for Homeland Security for TSA. These 37 machines will be integrated into airports' automated checked baggage conveyor systems. The new in−line EDS screening system will be a faster, more customer−friendly solution for screening 100 percent of all checked baggage for explosives. TSA is currently operating full in−line systems at eight airports in Boston, MA; Boise, ID; Manchester, NH; Jacksonville, FL; Lexington, KY; Orange County, CA; Tulsa, OK; and Tampa, FL. TSA is also operating an in−line EDS system for the international terminal in San Francisco, CA. The airports with an in−line system under construction are Seattle, WA; Dallas/Ft. Worth, TX; Las Vegas, NV, Denver, CO; Los Angeles, CA; Ontario, CA; Phoenix, AZ; Atlanta, GA; and Harrisburg, PA.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 00bcc9c

18. *June 30, Government Accountability Office* — **GAO−04−744: Surface Transportation: Many Factors Affect Investment Decisions (Report).** Passenger and freight traffic are expected to grow substantially in the future, generating additional congestion and requiring continued investment in the nation's surface transportation system. Over the past 12 years, the federal government has provided hundreds of billions of dollars for investment in surface transportation projects through the Intermodal Surface Transportation Efficiency Act of 1991 and its successor legislation, the Transportation Equity Act for the 21st Century. Reauthorization of this legislation is expected to provide hundreds of billions of dollars more in federal funding for surface transportation projects. This report provides information about the processes that state and regional transportation decision makers use to analyze and select transportation infrastructure investments. **The Government Accountability Office (GAO) identified (1) key federal requirements for planning and deciding on such investments, (2) how benefit−cost analysis facilitates sound decision making, and (3) other factors that decision−makers consider in evaluating and deciding on investments.** The Department of Transportation generally agreed with the report's contents and provided technical comments, which we incorporated as appropriate. Highlights:
http://www.gao.gov/highlights/d04744high.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−744

[Return to top]

Postal and Shipping Sector

19. *July 29, New Mexico Channel* — **Mail bomb in Albuquerque. A bomb scare sent Albuquerque, NM, police scrambling Wednesday, July 28, after a small device exploded in a resident's mailbox.** The police department received calls of an explosion before 5 a.m. Wednesday, around the time they believe the blast went off. The owner of the house said the device looked like a coffee can stuffed with newspaper and wrapped in duct tape. The Bureau of Alcohol, Tobacco and Firearms (ATF), bomb squad, and a bomb sniffing dog all searched the area, but found no sign of any other explosives. Police are still unsure whether the bomb was a prank or if someone intended to do serious harm.
Source: http://www.thenewmexicochannel.com/news/3588305/detail.html

20. *July 28, WTOL (OH)* — **Mail stolen from mailboxes.** Sylvania OH, residents are having their mail stolen from right out of their mailboxes. **The police say they dealt with over a dozen mail theft cases in the past month.** Detectives are urging residents to not put outgoing mail in their personal mailboxes, especially bills with checks in them. In each case the homeowner leaves checks in envelopes and then put the red flag up on the mailbox. **Someone is looking for those red flags, stealing the checks and getting easy access to the victim's account numbers**. Then, the thief goes to a bank, and deposits a check for a couple hundred dollars into the victim's account. Finally, the thief asks for cash back from the deposit.
Source: http://www.wtol.com/Global/story.asp?S=2103093

[Return to top]

Agriculture Sector

21. *July 29, Agricultural Research Service* — **New soybean line offers strong resistance. A new soybean line from the Agricultural Research Service (ARS) and the University of Missouri delivers a rare combination of resistance to two leading nematode pests.** The germplasm line, designated S99−3181, was initially bred for resistance to both soybean cyst nematode (SCN) and southern root−knot nematode by Grover Shannon, a soybean breeder at the University of Missouri's Delta Research Center. Prakash R. Arelli, a geneticist at the ARS Nematology Research Unit, identified S99−3181 for its resistance to SCN. Very few soybean lines, especially natto type, have this combination of broad nematode resistance and high yield potential, according to Arelli. In fact, during field trails, its yield was found to be equal to, or higher than, yields of Hutcheson, a popular cultivar. Additionally, the line also has shatter resistance, which means it will hold its seed after maturing. **The new line has broad resistance to SCN, the most destructive soybean pest in the U.S., causing annual losses as high as $438 million.** Root−knot nematodes are the second most destructive soybean pest in the southern United States. The line is expected to be used as a parent in breeding programs to develop new varieties that reduce soybean yield loss and reduce the need for pesticides.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

22. *July 29, Times−News (ID)* — **Blight found in second Idaho field. Potato blight has been found in two separate eastern Idaho fields this week, and experts expect the instance of the disease is more extensive.** "If we had these two independent experiences, it probably means well have more," disease specialist Jeff Miller said. Late blight, the fungus that caused the Irish potato famine in the 1850s, causes lesions on leaves that kill the potato plant and can spread at harvest to the tubers themselves, causing rot in storage. The two instances are not believed to be related, Miller said, and the farmers plan to destroy the affected parts of the fields to avoid further spread.
Source: http://www.magicvalley.com/news/business/index.asp?StoryID=5 820

23. *July 28, San Francisco Chronicle* — **Oak−killing disease found in New York. The discovery of a red oak tree in New York state infected with the disease known as sudden oak death could force changes in a nationwide quarantine of California nurseries as scientists re−evaluate the spread of the microbe.** The infected tree was found earlier this month inside the Tiffany Creek Preserve, a 192−acre nature park in Nassau County, nowhere near any nurseries that might have received diseased flora from California. **Forestry experts are at a loss to explain how the pathogen got to the preserve or how long it has been there.** The fungus−like organism, known scientifically as Phytophthora ramorum, has more than 60 host plants in the U.S., but has, until now, never been found in the wild outside of the coastal regions of Northern California and southern Oregon. An intensive survey of the Nassau County preserve, including DNA samples from every suspicious tree within a 20−acre section of forest, is being conducted to determine if the infestation is more widespread, according to Claude Knighten, spokesperson for the Animal and Plant Health Inspection Service.
Source: http://www.sfgate.com/cgi−bin/article.cgi?file=/c/a/2004/07/ 28/MNGOR7U81K1.DTL

24. *July 28, Agence France Presse* — **UN to recommend wider use of bird flu vaccine. Experts meeting in Thailand's capital will consider increased use of bird flu vaccines for chickens across Asia to try to tackle a resurgence of the deadly disease, the Food and Agriculture Organisation (FAO) said on Wednesday, July 28.** The chief of the United Nations' (UN) animal health service said it was shifting its position to back a wider use of injections to fight a virus that has left 24 people and 200 million chickens dead. "The FAO is going to give revised guidelines and we will be in some ways supporting more vaccination than before," Joseph Domenech said at a meeting here of top veterinary officials from Southeast Asia. **"They won't protect 100 percent against infection, and some vaccinated animals could carry the virus. But they will not contribute to outbreaks."** The FAO has recommended vaccination policies "where appropriate and practical" since the height of the crisis in February, but several nations including Thailand, the world's fourth largest poultry exporter, have banned vaccines until more thorough research is conducted. Key poultry populations that would be targeted include hens laying eggs for human consumption and young birds needed to replenish devastated poultry stocks. **"There will be more animals sick, more outbreaks, and more sources of the virus if there is no vaccine," said Domenech.**
Source: http://www.iol.co.za/index.php?set_id=1&click_id=143&art_id= qw109099908550B221

[Return to top]

Food Sector

25. *July 29, Toronto Star (Canada)* — **Water bottles ruled safe after tampering scare. Cases of bottled water delivered to two Toronto, Canada, modelling and talent agencies last week were tampered with after they were bought, Toronto police say.** One case of 12 bottles was delivered to Christen & Associates Model and Talent Management on July 22. A second case was delivered to Blitz Models and Talents. **A promotional letter had been attached to the product, but employees found tampering had occurred when they observed the bottles, and they called police.** Police are advising that the Nestle's Aberfoyle brand of bottled water is safe for the public to drink. The cases that were tampered with were sent to the Center of Forensic Sciences for examination. Detectives from the Toronto police department are still investigating. Police say any person or company receiving this type of promotional package should examine the contents before consuming and notify police if there are any concerns.
Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1091052613470&call_pageid=968350130169&col=969483202845

26. *July 28, Food Safety and Inspection Service* — **Ground beef patties recalled. Quaker Maid Meats, Inc., a Reading, PA, firm, is voluntarily recalling approximately 170,000 pounds of ground beef patties due to mislabeling.** The beef patties were partially made from Canadian product that was mislabeled and ineligible for import to the United States. The patties were produced on July 15, 16, 19, and 20 and were shipped to distribution centers and retail stores in Pennsylvania, New Jersey, Virginia, North Carolina, South Carolina, Florida, Wisconsin, and Maine.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_028_2004_Relea se/index.asp

27. *July 28, Food Production Daily* — **New E. coli research offers safer meat processing. Scientists at the University of Edinburgh, in collaboration with the Scottish Agricultural College and the Moredun Research Institute, have discovered that E. coli O157:H7 colonizes only the last few centimeters of the cattle gut.** As a result, bacteria are spread onto the surface of feces as they leave the cow and can easily contaminate the environment. In slaughterhouses, E coli can be transferred to meat if poor hygiene standards are observed. Therefore, eradicating deadly E. coli O157:H7 from the bottoms of cows may prevent future outbreaks of food poisoning. The majority of people with E. coli O157:H7, picked up the infection from cattle, either through direct contact with feces or by consuming contaminated meat or milk, according to an article in the August issue Microbiology Today. “We are focused on understanding where and how E. coli O157:H7 colonizes cattle,” said Dr David Gally from the University of Edinburgh. "Our aim is to produce vaccines that stop the bacteria from attaching themselves to the gut wall. This prevents colonization and therefore reduces the threat to human health from this pathogen."
Source: http://www.foodproductiondaily.com/news/news−NG.asp?id=53813

28. *July 28, Food and Drug Administration* — **FDA finds ground castor beans, not ricin, in tampered baby food. Contrary to the impression given by some early reports, the Food and Drug Administration (FDA) did not find purified ricin in two baby food jars involved in an apparent tampering case in the Irvine, CA, area.** To date no injuries have been

reported, and these problems seem to be isolated within the immediate Irvine area. FDA, which conducted the analyses of these products, found what appears to be the ground−up remnants of castor beans. Although ricin can be purified through chemical extraction processes from castor beans, the material found in these jars was far less toxic than purified ricin. Nevertheless, consumers who find anything suspicious concerning the packaging or contents of baby food products should not feed it to anyone, but instead notify their local FDA office.
Source: http://www.fda.gov/bbs/topics/news/2004/new01097.html

[Return to top]

Water Sector

29. *July 29, Modesto Bee (CA)* — **Dirt used to plug levee tainted. Dirt sold by the Port of Stockton and used to shore up a levee in the Sacramento−San Joaquin Delta, in California, contains toxic metals, which could leach into the water and threaten water safety standards, tests showed.** The soil, which contains heavy metals but does not qualify as hazardous waste, was sold by the Port of Stockton and used to strengthen a levee that borders Jones Tract, the low−lying delta island that flooded on June 3, The Record newspaper reported. Scientists said the metals present in the soil could impact the quality of the water in that part of the delta, but state and port officials downplayed the results, arguing that additional testing was needed, the Stockton paper stated. Water pumped from the delta irrigates about one million acres of farmland, and reaches about 22 million users as far away as Los Angeles. The port sold the dirt, which was left over after dredging waterways, to the state Department of Water Resources. The sediment was used to strengthen a 2 and a half mile section of the levee.
Source: http://www.modbee.com/local/story/8914374p−9806576c.html

[Return to top]

Public Health Sector

30. *July 29, Reuters* — **Mystery illness in Taiwan. One student at a Taiwan army college has died and 23 have fallen ill from a mysterious virus, but health officials said Thursday, July 29, it was unlikely to be Severe Acute Respiratory Syndrome.** The student at the college in southern Kaohsiung county suffered high fever and coughing before dying Saturday, July 24, Shih Wen−yi, acting director general of the Center for Disease control, said. **Eighteen of the 23 who came down with similar symptoms have already recovered but were being monitored in isolation from other students, said Shih.** No new cases have been reported since the death, said Shih.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=5809282

31. *July 29, Reuters* — **Dengue vaccine in development. A Malaysian bio−tech firm is developing a vaccine to prevent dengue fever, an infectious disease carried by mosquitoes that can be fatal, the company said Thursday, July 29.** Dengue fever, which is carried by the Aedes aegypti mosquito, infects about 50 million people worldwide every year. **A vaccine has never been developed.** The company said its vaccine, was being tested at the University of Malaya's teaching hospital. A professor at the university confirmed the vaccine had been sent

there for testing. The findings are due to be released in three months. Dengue fever afflicts victims mostly during and shortly after the rainy season in tropical and sub−tropical areas of Africa, Southeast Asia, China, India, the Middle East, Caribbean, and Central and South America, Australia, and the Pacific.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=5811966

[Return to top]

Government Sector

32. *July 29, Federal Computer Week* — **Intelligence officials clamor for information sharing.** Shock from the September 11, 2001, terrorist attacks has caused a near 180−degree shift in thinking about classified information, according to national security officials. Several current and former National Security Agency officials who spoke this week in Washington, DC, at GovSec, a government security conference, said sharing intelligence information with coalition partners must become the new way of doing business. **But changing data−handling techniques within intelligence agencies will require, among other things, new tools that allow analysts to share information. Current intelligence tools make sharing difficult because they were designed to be used in a highly restricted information culture, he said.** Besides new tools for handling intelligence data, new national security requirements will necessitate changes in current laws and policies that limit access to classified information to only those who meet the need−to−know standard, said Robert McGraw, technical director for information assurance at NSA. **NSA's researchers already have begun work on desktop PC prototypes that could start to simplify intelligence sharing by eliminating the clutter of multiple desktop workstations**, said Robert Meushaw, technical director for information assurance research at NSA.
Source: http://fcw.com/fcw/articles/2004/0726/web−intel−07−29−04.asp

33. *July 29, Garden City Life (NY)* — **New York Senate passes anti−terrorism legislation.** The New York State Senate passed legislation agreed upon by the governor, attorney general and both houses of the state legislature that would give New York the toughest, most comprehensive anti−terrorism laws in the nation. **The bill (S.7685), co−sponsored by Senator Kemp Hannon of Garden City, increases penalties for those who provide support to terrorists and supplies law enforcement officials with additional tools to prevent future terrorist attacks in New York State.** "This bill represents a step in the effort to make New York safer," Hannon said. "Enacting these measures now is crucial, given the threat of terrorist acts at the upcoming convention and during the fall elections." The legislation would strengthen existing laws by facilitating the investigation and prosecution of terrorists; create new anti−terrorism crimes; and severely punish the possession and use of chemical and biological weapons. Among other points, the legislation would create the crime of money laundering in the first, second, third and fourth degrees to help cut off money that fuels terrorism. And, it would create the crime of criminal possession and use of a chemical or biological weapon in the first, second and third degrees.
Source: http://www.antonnews.com/gardencitylife/2004/07/30/news/hann on.html

34. *July 28, Federal Computer Week* — **Geospatial comments sought. The Interior Department's U.S. Geological Survey is accepting public comments on Version 2 of the**

Geospatial One−Stop Portal. In May, officials at the Federal Geographic Data Committee's Homeland Security Working Group published the draft policy advising agency officials about striking the proper balance of access and security and ways to identify sensitive data. The group published the guidelines for federal and local governments, private−sector entities and not−for−profit organizations that create and maintain geospatial data. **According to the Office of Management and Budget, about 80 percent of all government information has a geographic component. Geospatial One−Stop and the Federal Geographic Data Committee support standardization and intergovernmental agreements on standards and interoperability for geospatial data.** One of the 24 e−government initiatives under the President's Management Agenda, Geospatial One−Stop is meant to be a central place for discovering and accessing distributed collections of Internet−accessible services data, maps, and geospatially enabled applications and Websites. Other objectives for the portal include making it a resource for agencies to discover potential cost−sharing partners for planned acquisitions. Officials want the portal to be accessible online at all times.
Source: http://fcw.com/fcw/articles/2004/0726/web−geospatial−07−28−0 4.asp

[Return to top]

Emergency Services Sector

35. *July 29, Associated Press* — **Squad cars swarm city blocks as part of counterterrorism drills.** The New York Police Department has been conducting counterterrorism drills in which dozens of squad cars descend upon a city block and quickly park with their rear tires against the curb in formation. "It's part of a counterterrorism overlay that is tweaked from time to time, based on conditions and intelligence," a police department spokesperson, Paul Browne, told The New York Times for its Thursday, July 29, editions. The drills, called critical response surges, have been held almost daily for the past month in various locations around the city, including outside the Metropolitan Museum of Art and on West 59th Street near Central Park. **Browne told the Times that the drills are taking place "frequently" and they are "not exclusively" in preparation for the Republican National Convention next month, but declined to give other details, such as how many cars take part in each surge.**
Source: http://www.newsday.com/news/local/wire/ny−bc−ny−−nypddrills0 729jul29,0,1691507.story?coll=ny−ap−regional−wire

36. *July 29, Platte County Sun (MO)* — **Area emergency personnel practicing to face terrorism.** About 100 emergency personnel, gathered for a bio−terrorism exercise at Platte City High School in Platte City, MO, focused on how to aid the sick and dying following a bio−terrorist attack. The mock attack released a pneumonic plague at Kemper Arena. The plague causes high fever, chills, headache and upper respiratory symptoms. The virus kills when untreated. **"We were one of seven sites chosen for this mass prophylaxis dispensing exercise," said Susan Hoskins, spokesperson, Platte County Health Department. "This tests our ability to do mass distribution of medicines for naturally occurring disease outbreaks or bio−terrorist attacks. The optimum number of patients we're shooting to treat today is 200 an hour."** "We're here for interior and exterior support," Platte City Police Chief Joe McHale said. "We are the first responders, handling crowd control, security." After the three−hour exercise, experts evaluated each triage site.
Source: http://www.zwire.com/site/news.cfm?newsid=12535289&BRD=1452&

PAG=461&dept_id=448709&rfi=6

[Return to top]

Information Technology and Telecommunications Sector

37. *July 29, Associated Press* — **Law enforcement tackling computer crime.** Federal and state law enforcement agencies are joining forces in Virginia to combat computer crimes, officials announced Thursday, July 29. The Cyber−Crime Strike Force will have a staff of seven investigators: four from the FBI, two from the state Attorney General Jerry Kilgore's office and one from the Virginia State Police. **They will work out of the Richmond FBI office, which has a computer lab from which online undercover investigations may be conducted.** Three attorneys from Kilgore's office and one from the office of U.S. Attorney Paul J. McNulty will prosecute the cases in state and federal courts. McNulty said that the partnership will help agencies share intelligence and bring computer criminals to justice more quickly. **Don Thompson, special agent in charge of the FBI in Richmond, said the strike force will go after hackers, scam artists, identity thieves, sexual predators and purveyors of child pornography.**
Source: http://www.nytimes.com/aponline/technology/AP−Computer−Crime s.html

38. *July 29, Government Computer News* — **PDAs—convenience, and no security.** A proof−of−concept virus discovered last week is a relatively benign bug for infecting Windows CE devices. It carries no destructive payload and has not been released in the wild. But a little tweaking of the code demonstrated at the Black Hat Briefings Wednesday, July 28, can let an attacker delete files from a personal digital assistant running the Microsoft operating system. **PDAs have not been obvious targets so far for virus writers and hackers, but their software carries most of the security vulnerabilities that have caused headaches on desktop and notebook computers.** Seth Fogie, vice president of Airscanner Corporation, demonstrated a number of hacks that would wipe data from the devices or let a snooper spy on the PDA while in use. The devices also provide what Fogie called mobile−attack platforms against wireless networks. He said network administrators should accept that the personal devices would be used on networks and make an effort to understand who is using them and how.
Source: http://www.gcn.com/vol1_no1/daily−updates/26760−1.html

39. *July 29, Computerworld* — **Search engines expose vulnerabilities.** Hackers have long used Internet search engines to parse through a Website's source code, seeking clues about what the site contains and configuration information that may be useful in launching an attack. Matt Fisher of SPI Dynamics Inc., said past software development practices for Websites often resulted in insecure code containing critical information. Hackers, using a Web browser and a search engine, frequently parse Websites looking for just such exposed nuggets of exploitable information. Web application vulnerabilities are not homogeneous, and every Website is unique, Fisher said. "You can't issue a patch for a Web application vulnerability. You've got to fix it yourself, and since Port 80 must be open, firewalls won't protect this type of vulnerability." **The recent MyDoom.O worm used search engines to find more e−mail addresses in targeted domains. Search engines would have to remove functionality to try to thwart hackers exploiting their caches**, Chris Wysopal of security assessment company

@stake Inc. said. **This wouldn't be feasible in today's competitive Internet marketplace**, which relies on powerful search engines to parse through the boundless information on the Internet.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,94880,00.html

40. *July 28, Check Point Software Technologies* — **Check Point plugs VPN security hole. An ASN.1 issue has been discovered affecting Check Point VPN−1 products during negotiations of a VPN tunnel which may cause a buffer overrun, potentially compromising the gateway.** In certain circumstances, this compromise could allow further network compromise. Check Point Software customers who do not use Remote Access VPNs or gateway−to−gateway VPNs, or who have upgraded to current product versions (VPN−1/FireWall−1 R55 HFA−08, R54 HFA−412, and VPN−1 SecuRemote/SecureClient R56 HF1) are not affected by this issue. A single packet attack is only possible if Aggressive Mode IKE is implemented. Check Point is not aware of any organizations that have been affected by this issue. However, in order to protect VPN−1 Gateways, **Check Point recommends that customers install an update on all enforcement modules.**
Source: http://www.checkpoint.com/techsupport/alerts/asn1.html

41. *July 28, Associated Press* — **Iowa company supplied Internet services for terrorists.** A technology company based in Cedar Falls, IA, discovered last week its Internet services were used as Websites operated by Islamic terrorist organizations. FBI Special Agent Jeff Tarpinian in Omaha, NE, confirmed Tuesday, July 27, that authorities had been contacted by FastServers.net officials. **The company provided wholesale Internet services through retail customers that were used by Arabic−language Websites operated by Hamas, a militant Palestinian group; by the Al−Aqsa Martyrs Brigade, which has been responsible for Middle East suicide bombings; and for message forums used by al Qaeda supporters.** All three sites have been shut down, Ian Andrusyk, the company's president, said. The company's servers used by the terrorist groups were in Fremont, CA. The relationship between the Iowa firm and the terrorist groups' Websites was reported last week by the Middle East Media Research Institute, a nonprofit organization based in Washington, DC. **The Websites were registered by individuals or organizations from Malaysia, Bulgaria and the Middle East**, the institute said.
Source: http://www.wcfcourier.com/articles/2004/07/28/business/local/0974e4e40015216286256edf004dfec0.txt

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: The latest variant of MyDoom created the unintended effect of creating a Denial of Service (DoS) condition in several Internet Search Engine Sites. This is due to the fact that the worm attempts to perform

internet searches for valid email addresses for domain names it finds on victim computers.

Current Port Attacks

Top 10 Target Ports	135 (epmap), 4899 (radmin), 137 (netbios−ns), 9898 (dabber), 1434 (ms−sql−m), 5554 (sasser−ftp), 445 (microsoft−ds), 3127 (mydoom), 1026 (nterm), 1023 (Reserved) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the

Subscription and Distribution Information:	DHS/IAIP Daily Report Team at (703) 883−3644. Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer